Notice of Allowability	Application No.	Applicant(s)	
	10/519,698	GIRAULT ET AL.	
	Examiner	Art Unit	
	Sarah Su	2431	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *pre-appeal brief conference request filed 16 February 2010*.

2. ☒ The allowed claim(s) is/are *1-4,6-13,15-18 and 20-30*.

3. ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☒ All b) ☐ Some* c) ☐ None of the:
      1. ☐ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
      3. ☒ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☒ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application
6. ☒ Interview Summary (PTO-413), Paper No./Mail Date *3/19/10* .
7. ☒ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

/Sarah Su/
Examiner, Art Unit 2431

NOTICE OF ALLOWANCE

1. Claims 1-4, 6-13, 15-18, and 20-30 are presented for examination.

Response to Arguments

2. Applicant's arguments with respect to claims 1-30 have been fully considered and are persuasive. The rejection of 18 November 2009 has been withdrawn.

Drawings

3. The drawings were received on 18 March 2010. These drawings are acceptable.

EXAMINER'S AMENDMENT

4. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Mark Bergner on 19 March 2010.

The application has been amended as follows:

a. Cancel claims 5, 14, and 19.

b. In claim 1, line 5: delete "generating, at the first entity" and insert -generating, on a processor at the first entity-;

c. In claim 1, after line 15, insert:

"wherein the second element of proof is generated by the first entity by subtracting, from the random integer, the private key multiplied by the common number,

wherein the linear combination equal to the second exponent comprises a positive unitary coefficient for the common number and a positive unitary coefficient for the public key exponent multiplied by the second element of proof, and

wherein, in the verified relationship, the first element of proof is considered with a unitary exponent power."

d. In claim 13, after line 15, insert:

"wherein the calculation means is designed to generate the second element of proof by taking the difference between the random integer and the private key multiplied by the common number or, where the common number is split into two elementary common numbers, by subtracting from the random integer multiplied by the first elementary common number, the private key multiplied by the second elementary common number."

e. In claim 15, line 1: delete "as claimed in claim 14" and insert –as claimed in claim 13–;

f. In claim 16, after line 14, insert:

"wherein the second element of proof is generated by the first entity by subtracting, from the random integer, the private key multiplied by the common number, wherein the linear combination equal to the second

exponent comprises a positive unitary coefficient for the common number and a positive unitary coefficient for the public key exponent multiplied by the second element of proof, and wherein, in the verified relationship, the first element of proof is considered with a unitary exponent power."

g. In claim 20, line 1: delete "as claimed in claim 19" and insert –as claimed in claim 1–;

h. In claim 22, line 1: delete "as claimed in claim 19" and insert –as claimed in claim 1–;

i. In the Abstract, line 2: delete "means of a private RSA key" and insert –use of a private RSA key–;

j. In the Abstract, line 2: delete "means of a public RSA key" and insert –use of a public RSA key–.

Allowable Subject Matter

5. Claims 1-4, 6-13, 15-18, and 20-30 are allowed.

6. The following is an examiner's statement of reasons for allowance:

Claim 1 discloses of "generating, on a processor at the first entity, a first element of proof by using a generic number raised to a first power, modulo the modulus, having a first exponent equal to the public key exponent multiplied by a random integer kept secret by the first entity, whereby calculation of said first element of proof is executable independently of the transaction." Claim 1 also discloses of "verifying, at the second entity, that the first element of proof is related through a relationship with a second

power, modulo the modulus, of a generic number having a second exponent equal to a linear combination of at least part of the common number and of the public key exponent multiplied by the second element of proof, wherein the second element of proof is generated by the first entity by subtracting, from the random integer, the private key multiplied by the common number, wherein the linear combination equal to the second exponent comprises a positive unitary coefficient for the common number and a positive unitary coefficient for the public key exponent multiplied by the second element of proof." These features, in combination with the other limitations in the claims, are not anticipated by, nor made obvious over, the prior art of record.

Claim 13 discloses of "calculation means for generating a first element of proof completely or partly independently of the transaction, said first element of proof being generated by said prover device by raising a generic number to a first power, modulo the modulus, having a first exponent equal to the public key exponent multiplied by a random integer kept secret by the prover device, and for generating a second element of proof related to the first element of proof and dependent on a common number specific to the transaction." Claim 13 also discloses of "wherein the calculation means is designed to generate the second element of proof by taking the difference between the random integer and the private key multiplied by the common number or, where the common number is split into two elementary common numbers, by subtracting from the random integer multiplied by the first elementary common number, the private key multiplied by the second elementary common number." These features, in combination

with the other limitations in the claims, are not anticipated by, nor made obvious over, the prior art of record.

Claim 16 discloses of "communication means for receiving a first element of proof, which includes at least the result of a first power, modulo the modulus, of a generic number raised to the power of a first exponent equal to the public key exponent multiplied by a random integer, and a second element of proof or a third element of proof, and for receiving or transmitting a common number specific to a transaction within which the first and the second or the third element of proof are received." Claim 16 also discloses of "calculation means for verifying that the first element of proof is related through a relationship, modulo the modulus, with a second power of the generic number having a second exponent equal to a linear combination of at least part of the common number and of the public key exponent multiplied by the second element of proof, wherein the second element of proof is generated by the first entity by subtracting, from the random integer, the private key multiplied by the common number, wherein the linear combination equal to the second exponent comprises a positive unitary coefficient for the common number and a positive unitary coefficient for the public key exponent multiplied by the second element of proof." These features, in combination with the other limitations in the claims, are not anticipated by, nor made obvious over, the prior art of record.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably

accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Conclusion

7. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

a. Endo et al. (US 2004/0148325 A1) discloses a system and method for employing the Chinese Remainder Theorem using modular calculations.

b. Kakchi et al. (US Patent 6,353,888 B1) discloses a system and method for access rights authentication.

c. Liskov et al. (US Patent 6,411,715 B1) discloses a system and method for verifying the cryptographic security of a selected private and public key pair without knowing the private key.

d. Shin et al. (US Patent 7,155,745 B1) discloses a system and method for providing data storage with user's access right.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Sarah Su whose telephone number is (571) 270-3835. The examiner can normally be reached on Monday through Friday 7:30AM-5:00PM EST..

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, William Korzuch can be reached on (571) 272-7589. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/William R. Korzuch/
Supervisory Patent Examiner, Art Unit 2431

/Sarah Su/
Examiner, Art Unit 2431